A prototype tool for information security awareness and training

S.M.Furnell, M.Gennatou and P.S.Dowland

ABSTRACT

Information systems security is a critical issue for all organisations with a significant dependence upon information technology. However, it is a requirement that is often difficult to address, particularly within small organisations, as a result of a lack of resources and expertise. This paper identifies the need for security awareness and describes the prototype implementation of a software tool that enables individuals to pursue self-paced security training. The tool provides an environment that permits the user to simulate the introduction of security into a number of pre-defined case study scenarios. This enables staff to become familiar with the types of countermeasures available, the situations in which they are appropriate and any constraints that they may impose. This would be particularly valuable in small organisations where specialist knowledge is often scarce and issues need to be addressed by existing staff.

KEYWORDS

Security Awareness, Security Training, Security Culture.

INTRODUCTION

The issue of information systems security is one that is faced in some form by all organisations in all sectors. Security is a multi-faceted problem, the comprehensive solution to which will normally encompass physical, procedural and logical forms of protection. As a result, a range of expertise is typically required to ensure that appropriate solutions can be realised. However, another characteristic is that many aspects of security are often transparent until a breach occurs. As such, a key issue is to ensure that security is given appropriate recognition within an organisation before problems have a chance to occur.

A security policy can only be effective if staff know, understand and accept the necessary precautions. This leads to the requirement for appropriate training and awareness within an organisation, in order to foster an appropriate security culture (Fowler, 1996). This paper considers the problems that may be faced in terms of fostering such a culture, particularly within small organisations (with less than 100 employees), where resources may be limited. It then proceeds to describe a prototype software tool that may be used as a means of assisting the understanding and use of security countermeasures.

THE PROBLEM OF PROMOTING SECURITY AWARENESS

Although security is a recognised issue, it is often found that organisations do not have a full understanding of what they should be doing or how to go about it. The availability and provision of comprehensive security guidelines is not the problem, as appropriate materials can be obtained from a number of sources. For example, in the UK, British Standard 7799 has been produced to guide the selection of baseline security measures within most organisations (British Standards Institution, 2000). The problem is instead one of ensuring that security awareness occurs both in the first instance and as an ongoing factor of an organisation's operation.

In an ideal situation, one would expect security issues and responsibilities to be highlighted and reinforced in various ways within an organisation. For example:

- Formal co-ordination of security by a nominated security administrator or administration team. A 1998 survey of information security practices within UK businesses reveals that the means by which the formal responsibility for security is handled is quite varied (KPMG, 1998). Only 24% claimed to have a security officer and, in most other cases, the issue of security often falls under the remit of IT or finance managers. Around 3% of respondents indicated that no one had formal responsibility.

- The inclusion of security-related issues as an integral part of any organisational training strategy and mechanisms to promote awareness during day-to-day activities.

- The facility for staff with key responsibilities, such as IT administrators, to attend specialist security training courses.

However, whilst the above may be practical within a large organisation, where staff capacity and financial resources can be specifically directed towards making these things a reality, the situation for small to medium sized establishments would rarely be so clear-cut. This is not to say that the security requirements or the sensitivity of data are any less within a small organisation and, in many cases, they will face the same challenges as larger companies. However, the perception of security within smaller organisations has been shown to be different. For example, the 1998 Business Information Security Survey, conducted by the UK National Computing Centre (NCC), asked respondents to rate the importance of security on a 5 point scale (where 5 indicated 'very important' and 1 indicated 'not important at all') (NCC, 1998). The average response from organisations with over 100 employees was 4.3. However, in organisations with fewer employees, there was marked contrast, with an average rating of 3.5. This attitude is further reflected by other findings in the same survey. For example, in terms of having a defined security policy document, 49% of medium to large organisations responded positively versus only 23% of organisations with less than 100 employees. In fact, even the larger organisations do not fare particularly well here (given the fundamental nature of a policy in guiding the security strategy), but it nonetheless illustrates the significant difference that exists depending upon the size of the organisation involved. It may be observed that these results date back to 1998, and it would be fair to raise the question of whether attitudes might have changed in the intervening period, alongside (for example) an increasing public

awareness regarding the security threat posed by the Internet. However, the executive summary of the most recent NCC survey suggests that a disparity continues to exist on the basis of organisational size, and states that "smaller organisations place limited value on information and its security" (NCC, 2000).

With the above in mind, it is necessary to consider why such a disparity exists in the first place. Part of the difference in attitude is likely to come from the operational constraints faced by smaller organisations, which will limit their potential to address security. Such constraints will include:

- not having staff with specific security expertise;
- lacking the financial resources to buy in specialist consultancy or provide training for their staff;
- lacking understanding of, or being dismissive of, the risks;
- inability or unwillingness to focus upon security due to other business priorities.

The need for specific attention to security within small systems has previously been recognised by the development of small-scale risk analysis approaches, such as ODESSA (Warren et al. 1997), which are cognisant of some of the above constraints. However, whilst such methods provide a means to select and guide the implementation of protection, they do little to actually increase the awareness and understanding of the underlying security technologies involved. As evidence of the problem, the respondents to the NCC's 2000 survey indicated that inadequate end user awareness was the most significant obstacle to information security, with over 55% citing it as a reason (ahead of issues such as budgetary constraints and technical complexity) (NCC, 2000). An explanation for this comes from the aforementioned KPMG survey, which indicated that only 31% of respondent organisations had security education and training programmes for their staff. Although this is again a low figure across the board, it is fairly safe to assume that the percentage relating to small organisations alone was lower still.

While there are numerous resources available to provide security advice and guidance without incurring significant expense (e.g. books, web sites, newsgroups and email lists), these do not offer the ability to test ones understanding in practice. It is desirable to be able to perform such testing before being faced with the task of applying security for real within an organisation. An environment is, therefore, required in which mistakes can be made and learnt from without incurring expense and leaving the system at risk. In response to this requirement, a security training tool is proposed that enables the investigation of available security countermeasures, combined with scenario-based testing and reinforcement. Such a tool represents an example of Computer Based Training (CBT) (Lee and Mamone, 1995).

The use of CBT has certain advantages over conventional methods, especially in company training scenarios. Firstly, CBT is proven to be cost-effective. After the initial set-up costs, what remains is a full-time training facility, available at all times within the organisation. It is also highly appropriate for staff trainees, as they are able to have control of their training and adjust it to their own personal needs. In this way, it is possible for employees to acquire the desired training in specific skills, at their own pace, without having to take time off from work. As such, the training process

can be tremendously flexible and personalised. It can also be used to train a large number of employees around the clock. It can run with minimal resource requirements, as there is much less need for a centralised training facility, and different companies or organisations can distribute the same CBT program among their employees.

A PROTOTYPE SECURITY TRAINING TOOL

A prototype tool has been implemented in Visual Basic in order to provide a functional proof of concept. The aim of the system is to provide a interactive and user-friendly approach to enhance user understanding of IT security. The system maintains two main repositories of information:

- A database of security countermeasures, with accompanying descriptions, which explain available security options and approaches.

- A selection of interactive scenario descriptions in which security countermeasures must be applied in order to solve one or more inherent security issues.

The information held regarding countermeasures encompasses the type of security issue that they aim to address, along with information about their suitability / strength and the associated impact upon the organisation and its staff (e.g. financial cost, ease of use, disruption to existing practices etc.) that their introduction would typically impose. Part of the exercise with the tool, when applying the countermeasures to the problem scenarios, is for users to consider these associated impacts. This is intended to ensure understanding of the fact that providing the highest possible level of security is rarely the only consideration. The level of protection must be commensurate with the value of the asset(s) requiring protection and must also be compatible with the environment in which they are placed. For example, in a college IT room (one of the example scenarios provided in the prototype system), fingerprint-based authentication would provide a high level of login security to prevent unauthorised access to the machines. However, the cost of deploying fingerprint scanners on each machine would probably not be merited by the sensitivity of the student materials to which they give access.

The system offers three modes of operation:

- Exploration mode – the user can interrogate the countermeasure database to learn more about different types of security.

- Evaluation mode – the user can test their understanding of security by applying countermeasures to the example scenarios.

- Author mode – allows the creation of new scenarios and the specification of the appropriate countermeasures to solve them. A scenario will typically be associated with a picture to illustrate it and all the relevant information will be kept in the scenario database. This mode would be utilised by appropriate security experts (who would not necessarily reside within the same organisation in which the tool is deployed for use).

The main mode of operation from the training perspective is the evaluation mode. This presents the user with a scenario and the security issues to be considered. The user is then be required to specify the optimal countermeasure arrangement to reduce the risks, by selecting protection for each of the problems identified. The system would then evaluate the overall security strategy that has been suggested, identifying any remaining weak areas or problems that might be introduced as a result.

Figure 1 depicts an example of a security scenario, as presented to the user. Rather then simply provide a case study description and ask the user to recommend countermeasures, it was considered that the activity would be more engaging for the user if they could begin by exploring the problem scenario and identify areas of weakness.

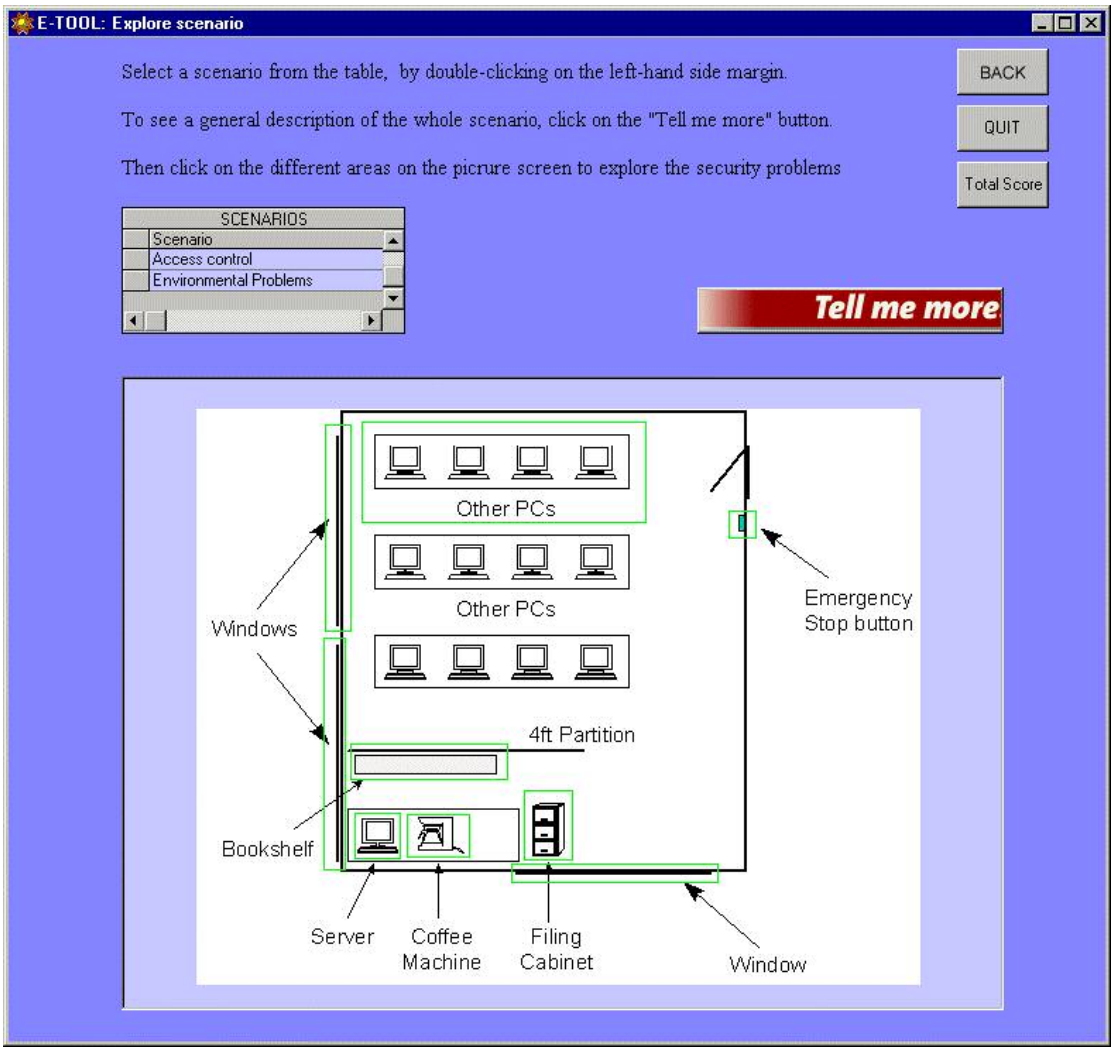

Figure 1 : An example security scenario

The user is able to explore the scenario by clicking on the highlighted areas of the image. Doing so reveals further elements of description regarding that aspect of the current scenario, which may or may not give a clue as to a particular security risk that needs to be addressed. An example of such an additional description is given in figure 2. In this case, the supplementary information is provided as a simple textual

description. However, this need not necessarily be the case and, in some scenarios, the author may choose to include another image (which may itself have further sub-elements to be explored) or other media, such as audio or video segments, to provide the necessary information.

If the user considers that a security problem exists, then they can proceed to the next stage of selecting appropriate countermeasures (note: in the description provided in figure 2, there is a problem in the sense that the uncontrolled access brings with it the risk of viruses and the described solution of allowing students to voluntarily check their disks on the server is not adequate and, indeed, puts the server at greater risk). If an incorrect assessment is made (e.g. the user believes there to be no problem when in fact there is one, or vice versa), then the overall score is affected accordingly, before the system then automatically guides the user in the correct direction.

Figure 3 depicts the countermeasure selection process. The main categories are shown on the left of the image, with the individual measures listed on the right. Users are able to select from different categories and obtain descriptions of the individual countermeasures therein. From this, they would be able to make a judgement as to whether the countermeasure is applicable to the scenario currently under consideration.

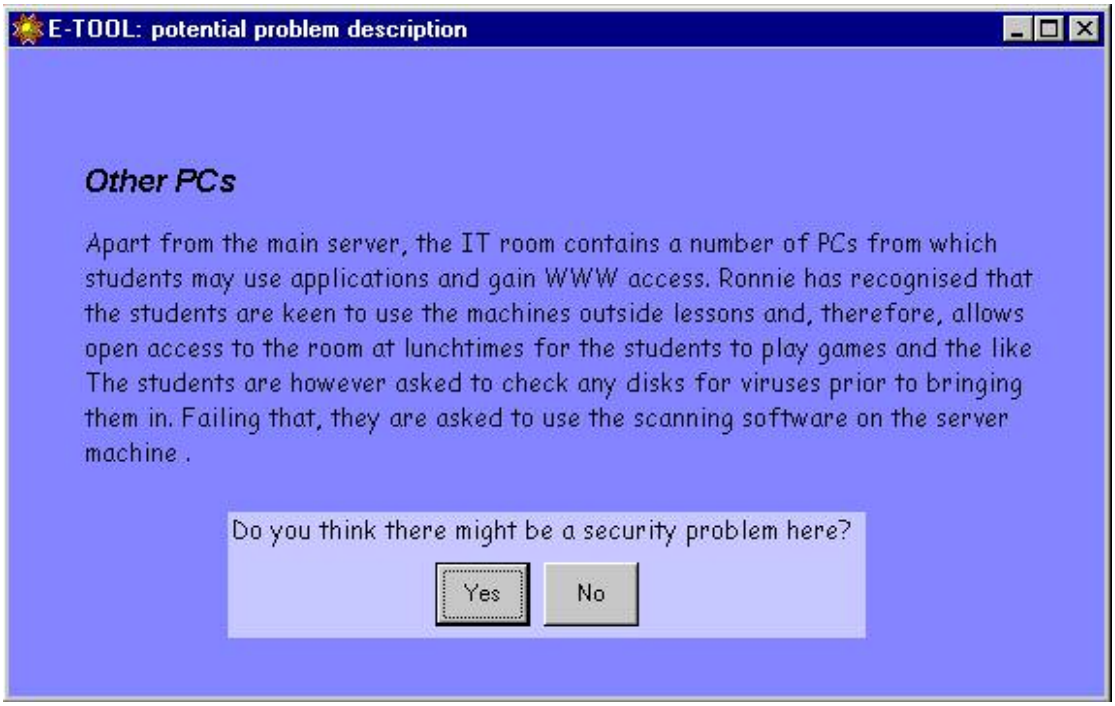

Figure 2 : A description of a potential problem area

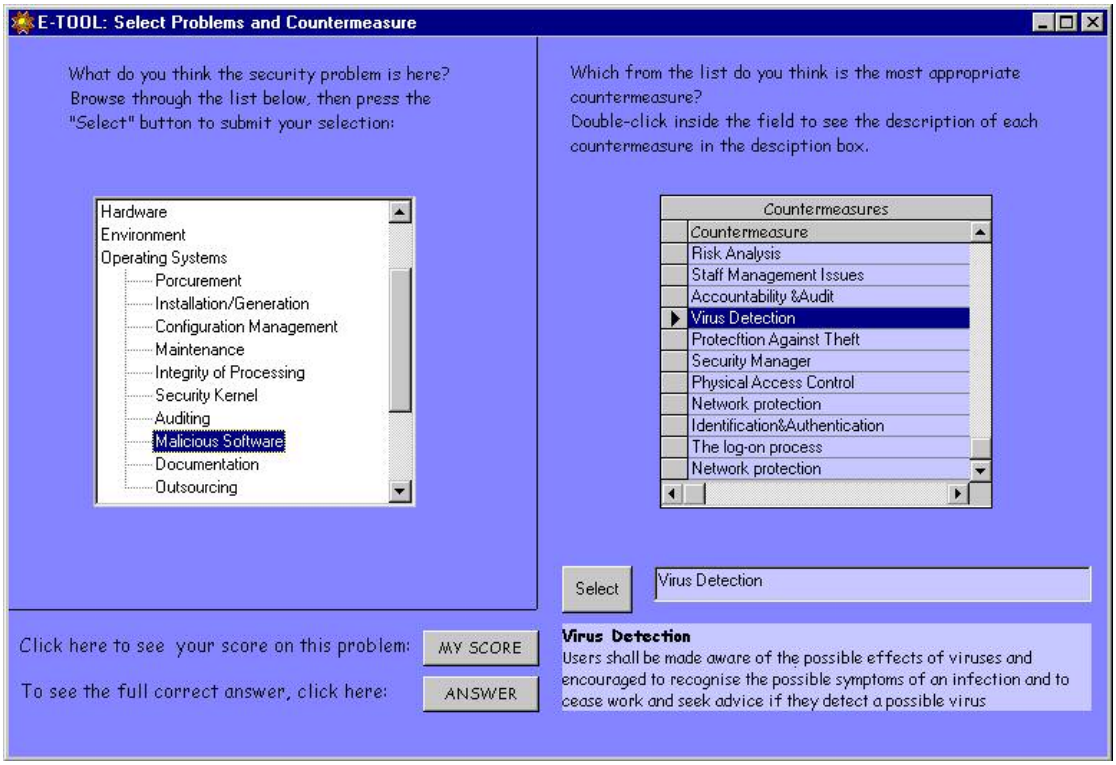

Figure 3 : Specifying appropriate countermeasures

Following the selection of the chosen countermeasures, the user is able to have their solution rated by the system against the optimum solution originally conceived by the author of the problem scenario. Through this they will be able to determine the appropriateness of their recommendations. If desired, the system could present additional information, such as a narrative description, to support the countermeasure solutions and ensure that the user understands the rationale behind the scenario author's approach. In some cases, there may be more than one valid solution, via different combinations of countermeasures that achieve the same objectives. The system would be able to assess this by comparing the attributes of the countermeasures chosen (e.g. protection category, disruption level, financial cost, user friendliness) with the attributes of those selected by the scenario author. These attributes are maintained in the countermeasure database along with the basic title and description details.

The current implementation of the tool is quite basic in terms of the number of example scenarios that have been developed. In practice, the success of the tool will depend upon there being a range and variety of problem scenarios to be solved. The usefulness from a training perspective is to expose users to different problems and then enable them to take the knowledge gained in one scenario and use it in the next.

Although not realised in the current implementation, it is conceivable that scenarios could be classified into different levels of difficulty, enabling a phased approach in which users are required to demonstrate proficiency in basic concepts before moving on to more substantial and subtle problems. In addition, scenarios could be topic focused, such that if the user believes they have a particular class of security issue to address within their organisation (e.g. relating specifically to authentication), then they could use the system to present them with problem scenarios targeted at this area.

Further development of the system is currently ongoing within the authors' research group. One additional option that is currently being investigated, in conjunction with the issues above, is the feasibility of replacing the prototype front-end with a web interface, which would lend itself to the deployment of the system within an organisational intranet environment.

CONCLUSIONS

Awareness of information security risks is a necessary requirement for any organisation utilising IT systems. However, as the paper has identified, the extent to which organisations are able to give focus to the issue is often influenced by practical considerations.

Although it does not remove all of the potential barriers to the introduction of security (e.g. cost of countermeasures), a tool such as that described makes a useful contribution by providing a context in which users can learn about security in a more active sense than simply reading reference material. They can also experiment with different security configurations, without financial or disruptive impacts upon their organisation. The proposed approach is not limited to application within small organisations, but is considered to be particularly suited to these environments, as operational constraints may preclude other alternatives.

REFERENCES

British Standards Institution. (2000). Information technology. Code of practice for information security management. BS ISO/IEC 17799:2000. 15 February 2001. ISBN 0 580 36958 7

Fowler J. (1996), "Developing The Security Culture At The SEISMED Reference Centres". In: B. Barber et al, editors. Towards Security in Medical Telematics: Legal and Technical Aspects. IOS Press, Amsterdam, pp.156-161.

KPMG. (1998), Information Security Survey 1998. KPMG Information Risk Management, London, UK. http://www.kpmg.co.uk/

Lee, W.W. and Mamone, R.A. (1995), The Computer Based Training Handbook: Assessment, Design, Development, Evaluation. Englewood Cliffs, NJ: Educational Technology Publications.

NCC. (1998), BISS '98 – Information Secuity, The True Cost To Business. National Computing Centre, Manchester, UK. http://www.ncc.co.uk/

NCC. (2000), The Business Information Security Survey 2000 (BISS 2000). National Computing Centre, Manchester, UK. http://www.ncc.co.uk/

Warren, M.J.; Furnell, S.M. and Sanders, P.W. (1997), "ODESSA : A new approach to healthcare risk analysis", in Information Security in Research and Business, L.Yngstrom and J.carlsen (eds.), Chapman & Hall, pp.391-402.